document to see if they make a specific reference to statistical analysis methods on the MIB. 16:51:05 16:51:23

I -- I mean there is some preliminary mention of intrusion detection off the MIB in page 15, the middle paragraph. My impression was that in reading -- well, when I read this, I really wasn't informed to specifically how they proposed to do statistical intrusion detection off the MIB, statistical analysis off the MIB. It's largely -- I mean if you look at page 15, this is the kind of thing I remember. It's largely a suggestion, which is at the time talking about the impediments for doing real-time statistical analysis using SNMP and suggesting that the working group in IETF modify how it does logging to facilitate -- to facilitate statistical analysis intrusion detection off a MIB. 16:51:43 16:51:49 16:51:59 16:52:04 16:52:10 16:52:15 16:52:28 16:52:32 16:52:40 16:52:50 16:52:57 16:53:03 16:53:15 16:53:28

So the answer to your question is I don't precisely know based on reading of the document what they could mean or what they could suggest as the kind of statistical analysis techniques would be in the box in the upper left. 16:53:31 16:53:34 16:53:37 16:53:42 16:53:42

BY MS. MOEHLMAN: 16:53:44

Q. What is it about the information in the patent specification on the alerts that are generated by lower level monitors that enables you to determine 16:53:47 16:53:53

UNITED STATES DISTRICT COURT

DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC.,
a California corporation,

Plaintiff and
Counterclaim-Defendant,

vs.

INTERNET SECURITY SYSTEMS, INC., a Delaware corporation; INTERNET SECURITY SYSTEMS, INC., a Georgia corporation; and SYMANTEC CORPORATION, a Delaware corporation,

Defendants and
Counterclaim-Plaintiffs.

CERTIFIED COPY

CASE NO: 04-1199 (SLR)

DEPOSITION OF GEORGE KESIDIS
VOLUME II

DATE:	Friday, May 26, 2006
TIME:	9:00 A.M.
LOCATION:	DAY, CASEBEER, MADRID & BATCHELDER 20300 Stevens Creek Boulevard Suite 400 Cupertino, CA 95014
REPORTER:	Patricia Hope Sales, CRR CSR License Number C-4423

8705
21418

Bell & Myers
CERTIFIED SHORTHAND REPORTER, INC.

50 AIRPORT PARKWAY, SUITE 205, SAN JOSE, CALIFORNIA 95110, TELEPHONE (408) 287-7500, FAX (408) 294-1211

a statistical detection method for intrusion detection? 14:18:51 14:18:55

A. No. 14:18:56

Q. Were Mr. Porras and Mr. Valdes the first to use a statistical detection method on network traffic data? 14:18:56 14:18:59 14:19:03

MR. POLLACK: Objection. Vague and ambiguous. 14:19:06

THE WITNESS: No. 14:19:08

BY MR. GALVIN: 14:19:09

Q. Were Mr. Porras and Mr. Valdes the first to use a signature detection method for intrusion detection? 14:19:09 14:19:12

MR. POLLACK: Same objection. 14:19:17

THE WITNESS: I'm just rethinking the previous question. 14:19:26 14:19:27

A statistical detection method on network data. I mean the course of your questions, I'm trying to parse the entire noninfringement story. I'm just having a hard time. 14:19:27 14:19:36 14:19:39 14:19:43

Okay. I -- I would say I believe the answer is no to the previous question. 14:19:46 14:19:48

And with regard signatures, I believe the answer is no more confidently. 14:19:50 14:19:54

THE VIDEOGRAPHER: Counsel -- 14:19:58

BY MR. GALVIN: 14:19:59

Q. One last question: Were Mr. Porras and 14:19:59

Mr. Valdes the first to de- -- use a signature detection method on network traffic data? 14:20:01 14:20:03

MR. POLLACK: Objection. Vague and ambiguous. 14:20:07

THE WITNESS: I would say generally speaking, no. 14:20:08 14:20:10

MR. GALVIN: Okay. Let's take a break. 14:20:11

THE VIDEOGRAPHER: We are going to go off the record. The time is 2:20 P.M. 14:20:12 14:20:13

This marks the end of tape number two in the deposition of George Kesidis. 14:20:16 14:20:18

(Recess.) 14:37:00

(Whereupon, Mr. Godfrey is not present in the conference room.) 14:37:00 14:37:01

THE VIDEOGRAPHER: We are back on the record. The time is 2:37 P.M. 14:37:01 14:37:02

This marks the beginning of tape number three in the deposition of George Kesidis. 14:37:04 14:37:07

BY MR. GALVIN: 14:37:09

Q. Dr. Kesidis, were Mr. Porras and Mr. Valdes the first to describe deploying more than one monitor in an enterprise network? 14:37:09 14:37:13 14:37:18

MR. POLLACK: Objection. Vague and ambiguous. 14:37:20

THE WITNESS: No. 14:37:21

BY MR. GALVIN: 14:37:24

Q. Were Mr. Porras and Mr. Valdes the first to 14:37:24

describe invoking countermeasures to a suspected attack on a computer network? 14:37:28 14:37:32

MR. POLLACK: Objection. Vague and ambiguous. 14:37:34

(Whereupon, Mr. Godfrey returned to the conference room.) 14:37:35 14:37:37

THE WITNESS: No. 14:37:37

BY MR. GALVIN: 14:37:38

Q. Were Mr. Porras and Mr. Valdes the first to describe monitoring a network for data transfers? 14:37:38 14:37:41

MR. POLLACK: Objection. Vague and ambiguous. 14:37:45

THE WITNESS: No. 14:37:46

BY MR. GALVIN: 14:37:48

Q. Were Mr. Porras and Valdes the first to describe building statistical profiles based on data transfers? 14:37:48 14:37:52 14:37:57

MR. POLLACK: Objection. Vague and ambiguous. 14:37:58

THE WITNESS: I -- I don't believe so, no. 14:38:23

BY MR. GALVIN: 14:38:26

Q. Were Mr. Porras and Mr. Valdes the first to monitor computer networks for errors? 14:38:26 14:38:28

MR. POLLACK: Objection. Vague and ambiguous. 14:38:32

THE WITNESS: No. 14:38:34

BY MR. GALVIN: 14:38:35

Q. Were Mr. Porras and Valdes the first to build statistical profiles based on errors on computer 14:38:35 14:38:39

networks? 14:38:42
MR. POLLACK: Same objection. 14:38:43
THE WITNESS: I -- I don't believe so, no. 14:38:46
BY MR. GALVIN: 14:38:51
Q. Were Mr. Porras and Mr. Valdes the first to monitor a network for network packet data volume for use in connection with intrusion detection? 14:38:51 14:38:55 14:38:59
MR. POLLACK: Objection. Vague and ambiguous. 14:39:03
THE WITNESS: No. 14:39:13
BY MR. GALVIN: 14:39:14
Q. Were Mr. Porras and Mr. Valdes the first to monitor a network for network connection denials for use in connection with intrusion detection? 14:39:14 14:39:18 14:39:23
MR. POLLACK: Objection. Vague and ambiguous. 14:39:35
THE WITNESS: Again, interpreted broadly, no. 14:39:41
BY MR. GALVIN: 14:39:44
Q. Were Mr. Porras and Mr. Valdes the first to monitor a network for error co- -- errors for use in connection with intrusion detection? 14:39:44 14:39:46 14:39:52
MR. POLLACK: Objection. Vague and ambiguous, asked and answered. 14:39:55 14:39:56
THE WITNESS: No, interpreted broadly. 14:40:00
BY MR. GALVIN: 14:40:03
Q. Do you consider the work described in the patents in suit to have revolutionized the field of 14:40:03 14:40:05

intrusion detection? 14:40:10

MR. POLLACK: Objection. Vague and ambiguous. 14:40:13

THE WITNESS: I don't know that I would use the word "revolutionized," but I believe that the inventions were a significant contribution to the art. I just -- I don't know that I would use the word "revolutionized." 14:40:17 14:40:18 14:40:28 14:40:34 14:40:39

BY MR. GALVIN: 14:40:40

Q. How would you define something that it -- to be a significant contribution to the art? 14:40:40 14:40:45

A. I think that speaking generally, if it solves an -- or if it answers an important problem. Sometimes the problem is a known problem; sometimes it's -- you know, hasn't been clearly defined, but if it -- if it addresses an important problem and addresses it -- addresses it well, then I would consider that a significant contribution to the art. 14:40:48 14:41:05 14:41:19 14:41:24 14:41:31 14:41:40 14:41:43

Q. And you believe that the work that's described in the patent specification satisfies that standard? 14:41:46 14:41:50

A. I believe so, yes. 14:41:53

Q. Is the EMERALD system that's described in the -- in the patent specification widely heralded or cited in the field of intrusion detection as an important contribution to the development of the art? 14:41:56 14:42:01 14:42:08 14:42:11

MR. POLLACK: Objection. Vague and ambiguous, 14:42:16

lacks foundation. 14:42:17

THE WITNESS: The -- the EMERALD system as described in the specification, I don't know that I have seen EMERALD cited by patent, but I have seen EMERALD cited quite frequently -- in my research on IDS I have seen it cited quite frequently. 14:42:19 14:42:24 14:42:27 14:42:32 14:42:41

BY MR. GALVIN: 14:42:44

Q. In November 19- -- prior to November 1998 what were the leading centers for development of intrusion detection -- the intrusion detection field? 14:42:44 14:42:48 14:42:52

MR. POLLACK: Objection. Vague and ambiguous, overly broad. 14:42:56 14:42:57

THE WITNESS: My understanding of some primary areas of development in intrusion detection -- do you mean academic or corporate or -- 14:42:58 14:43:01 14:43:09

BY MR. GALVIN: 14:43:12

Q. Either. 14:43:12

A. Some of them included certainly -- certainly Symantec and ISS would be included in that category. UC Davis. I'm referring to network intrusion detection. I don't have as much knowledge on -- on other contexts of intrusion detection, but network intrusion detection I would think Davis, SRI. And there were other researchers of note in this area, such as -- important centers. Let's see. 14:43:14 14:43:18 14:43:23 14:43:31 14:43:43 14:43:47 14:43:51 14:43:57

operating system, or both? 14:55:35

MR. POLLACK: Same objections. 14:55:38

THE WITNESS: TCP dump is a -- is a process 14:55:45

through which you can make a rather -- rather raw, 14:55:49

nonselective dump of every packet that you observe, 14:55:58

say, going by a wire. So you may have a -- a -- you 14:56:02

may have a net flow process which is computing net flow 14:56:09

information in a router, and although I don't know of a 14:56:13

specific instance, you can also have a TCP dump process 14:56:16

which is simply logging all the packets that go by 14:56:20

and -- specifically their headers, and recording them. 14:56:24

I believe there is a time stamp as well. So 14:56:29

there is a -- there is a temporal aspect to when the 14:56:32

packet whizzed by that may not be on the packet itself 14:56:38

is what I'm trying to say. 14:56:41

BY MR. GALVIN: 14:56:43

Q. Can a TCP dump be exported into a file, 14:56:43

computer file? 14:56:45

A. Oh, yeah, it is a file. It would be a file. 14:56:46

Q. And if a -- let's just turn to the '212 14:56:49

patent -- 14:56:54

A. Oh. 14:56:55

Q. -- which is Exhibit 7, for example. 14:56:55

Actually, I'm sorry, the '338 patent -- 14:57:03

A. Sure. 14:57:05

Q. -- which is Exhibit 4. And if you look at the first limitation. 14:57:06 14:57:20

A. Are you looking at -- 14:57:21

Q. Claim one -- 14:57:22

A. Sure. 14:57:23

Q. -- of the '338. 14:57:23

A. Right. 14:57:24

Q. "Receiving network packets handled by a network entity." 14:57:25 14:57:27

A. That's correct, yes. 14:57:28

Q. Would in your opinion -- well, withdraw that. 14:57:30

Sticking with claim one of the '338 patent -- 14:58:04

A. Okay. I'm there. 14:58:08

Q. -- what is your understanding of the meaning of the, well, phrase "network surveillance" in the context of the -- 14:58:11 14:58:14 14:58:20

(Reporter clarification.) 14:58:21

BY MR. GALVIN: 14:58:21

Q. -- "surveillance" in the context of the preamble of claim one? 14:58:21 14:58:21

A. Surveillance. 14:58:23

MR. POLLACK: Objection. Asked and answered. 14:58:28

THE WITNESS: The -- the preamble elaborates on what it means by "network surveillance," "receiving network packets handled by a network entity." 14:58:38 14:58:41 14:58:45

BY MR. GALVIN: 14:58:57

Q. Is it your opinion that the phrase "network surveillance" in the preamble is describing the purpose or intended use of this method? 14:58:57 14:58:59 14:59:03

MR. POLLACK: Objection. Vague and ambiguous. 14:59:06

THE WITNESS: It's a specific kind of network surveillance whose -- whose ultimate purpose is intrusion detection. 14:59:24 14:59:33 14:59:35

BY MR. GALVIN: 14:59:37

Q. And is the specific kind of network surveillance the method of network surveillance which is specified by the limitations that follow the preamble? 14:59:37 14:59:40 14:59:42 14:59:45

MR. POLLACK: Objection. Vague and ambiguous. 14:59:47

THE WITNESS: Yes. 14:59:52

BY MR. GALVIN: 14:59:54

Q. Is it your opinion that the phrase "network surveillance" -- or let me withdraw that. 14:59:54 15:00:00

Is it your opinion that the method which is claimed in claim one of the '338 patent would encompass network surveillance on any kind of computer network or a particular kind of computer network? 15:00:03 15:00:06 15:00:15 15:00:19

MR. POLLACK: Objection. Vague and ambiguous, asked and answered. 15:00:23 15:00:23

THE WITNESS: I think it's a particular kind of 15:00:42

computer network. 15:00:47
BY MR. GALVIN: 15:00:49
Q. And -- and what kind of particular kind of 15:00:49
computer network is claim one of the '338 patent 15:00:50
limited to? 15:00:54
A. I think -- 15:00:56
MR. POLLACK: Same objections here. 15:00:57
THE WITNESS: Sorry. 15:01:00
I think those that possess network entities 15:01:00
as -- as laid out in the specification. 15:01:08
BY MR. GALVIN: 15:01:14
Q. Okay. So if a computer network does not have 15:01:14
one of the network entities that is specified in the 15:01:19
claim, then it would be outside the scope of '338, 15:01:24
claim one? 15:01:31
MR. POLLACK: Objection. Vague and ambiguous. 15:01:47
THE WITNESS: Pardon me a second. I need to 15:01:47
just refresh my memory as to -- 15:01:49
MR. POLLACK: Can I hear that question again? 15:01:53
(The record was read as follows: 15:02:08
"Q. Okay. So if a computer 15:01:14
network does not have one of the 15:01:16
network entities that is specified 15:01:20
in the claim, then it would be 15:01:23
outside the scope of '338, claim 15:01:27

one?") 15:01:31

THE WITNESS: (Reviewing document(s).) 15:03:13

I -- I believe so. I mean I -- I believe 15:03:13

that's correct. I'm not sure, because up until now I 15:03:26

haven't really considered what a network might be that 15:03:33

didn't have a router in it or -- I believe so. 15:03:35

BY MR. GALVIN: 15:03:50

Q. Okay. I believe -- is it your opinion -- you 15:03:50

may have stated this already, but I want to be clear. 15:03:53

Is it your opinion that the phrase "network 15:03:57

entity" in claim one of the '338 patent is limited to a 15:04:02

gateway router or proxy? 15:04:08

MR. POLLACK: Objection. Mischaracterizes 15:04:13

testimony, asked and answered. 15:04:14

THE WITNESS: The specification refers to other 15:04:17

examples of what network entities may be. 15:04:29

BY MR. GALVIN: 15:04:32

Q. And what other examples does the specification 15:04:32

refer to? 15:04:35

A. In column two it refers to a VPN. 15:04:35

In -- in figure two, for example, it refers to 15:04:42

a firewall as another potential network entity. 15:04:50

I -- off the top of my head, I don't have an 15:05:00

exhaustive list from the spec, but at least those two 15:05:04

additional kinds of network entities. 15:05:10

UNITED STATES DISTRICT COURT

DISTRICT OF DELAWARE

CERTIFIED COPY

SRI INTERNATIONAL, INC., a California corporation

Plaintiff and Counterclaim-Defendant,

vs.

Case No. 04-1199 (SLR)

INTERNET SECURITY SYSTEMS, INC., a Delaware corporation; INTERNET SECURITY SYSTEMS, INC., a Georgia corporation; and SYMANTEC CORPORATION, a Delaware corporation,

Defendants and Counterclaim-Plaintiffs.

/

DEPOSITION OF GEORGE KESIDIS
VOLUME III

DATE: May 29, 2006

TIME: 9:00 a.m.

LOCATION: DAY CASEBEER MADRID & BATCHELDER
20300 Stevens Creek Boulevard, Suite 400
Cupertino, CA 95014

REPORTED BY: KAREN L. BUCHANAN, CSR No. 10772

8714
21420

Bell & Myers
CERTIFIED SHORTHAND REPORTER, INC.

50 AIRPORT PARKWAY, SUITE 205, SAN JOSE, CALIFORNIA 95110, TELEPHONE (408) 287-7500, FAX (408) 294-1211

Q. Well, could you just -- let's take this in two parts. 12:08:37 12:08:40

A. Let me just try to think of your question more carefully. You said one of ordinary skill looks at the claim language and looks at network packet data volume, and what do they interpret that to mean, given the spec? 12:08:41 12:08:45 12:08:49 12:08:53 12:08:55

Q. What's their definition? 12:08:56

MR. POLLACK: Objection. Vague and ambiguous. 12:09:05 12:09:05

THE WITNESS: I think that that phrase would be informed by the paragraphs in column 13 in 5 that we have been referring to. And the phrase -- the paragraph in column 13 is -- in my opinion teaches a more selective measure than the total packet volume, all of the observed packets, all of the packets observed by the sensor. 12:09:16 12:09:17 12:09:25 12:09:30 12:09:34 12:09:44 12:09:46

BY MR. GALVIN: 12:09:46

Q. And so what are the selected set of packets that are measured by the term "network packet data volume" as used in the patent, according to you? 12:09:47 12:09:51 12:09:54

A. Again, if it's -- if you're -- for example, in column 13, monitoring -- sorry, I'm fixated on one part. What they refer to as discarded packets. 12:09:58 12:10:05 12:10:45

(Reading document.) 12:11:01

So the example they gave of you're observing ICMP echoes that may result due to IP address scanning, you may be counting the number of such echoes. That would be a measure of a certain kind of volume. 12:11:37 12:11:49 12:11:59 12:12:04 12:12:04

Q. That's an example of a network packet data volume, correct? 12:12:12 12:12:15

MR. POLLACK: Objection. Vague and ambiguous. 12:12:17 12:12:28

THE WITNESS: As a data volume? Well, I'm not sure that that would -- that may be a measure of a transfer error, in fact. 12:12:29 12:12:52 12:13:08

BY MR. GALVIN: 12:13:08

Q. How about -- 12:13:14

A. It could be -- one possibility, drawing from column 5, and I'm just doing a hypothetical here, there could be -- so if you consider packets targeting ports to which an administrator has not assigned any network service, the number of such packets could be -- those may not necessarily result in the transfer error of any kind. The number of such packets, the volume of such packets could be -- sorry, the number of such packets could be a measure that's built. 12:13:15 12:13:18 12:13:27 12:13:40 12:13:44 12:13:53 12:13:57 12:14:00 12:14:05

Q. How about the total number of packets sent over an interval of time from a specific source IP 12:14:08 12:14:13

address, would that constitute a network packet data volume as claimed in claim 1 of the '203 patent? 12:14:20 12:14:23

MR. POLLACK: Objection. Vague and ambiguous. 12:14:26 12:14:35

THE WITNESS: So can you just clarify what the measure is a little bit? 12:14:36 12:14:37

BY MR. GALVIN: 12:14:37

Q. Sure. Total number of packets sent over an interval of time from a specific source IP address. Would that constitute a network packet data volume? 12:14:39 12:14:42 12:14:46

MR. POLLACK: Same objections. 12:14:51

THE WITNESS: I'm not sure that that specific example is taught in the patent specification. 12:15:14 12:15:16

BY MR. GALVIN: 12:15:16

Q. Well, I want to separate out -- is it your understanding that these categories are limited to the specific examples taught this the specification? 12:15:22 12:15:25 12:15:27

A. I'm sorry. What was your question? What context were you asking your question? 12:15:32 12:15:35

BY MR. GALVIN: 12:15:35

Q. My question was in the context of claim 1 of the '203 patent, is the total number of packets sent over an interval of time from a specific source IP address an example of a measure of network packet data volume? 12:15:35 12:15:37 12:15:44 12:15:49 12:15:53

MR. POLLACK: Objections. 12:15:54

THE WITNESS: To the extent that in column 5, they talk about -- of '338, event streams may also be based on packet source addresses. I don't think the intent, but it's possible that a special case could be a specific source address. 12:15:58 12:16:04 12:16:11 12:16:25 12:16:28

BY MR. GALVIN: 12:16:28

Q. So is the total number of packets sent over an interval of time from a specific source IP address an example of a measure of network packet data volume as claimed in claim 1 of the '203 patent? 12:16:32 12:16:35 12:16:38 12:16:41

MR. POLLACK: Objection. Vague and ambiguous, asked and answered. 12:16:44 12:16:46

THE WITNESS: In the context of column 5, I would say -- I would say yes. 12:16:49 12:16:51

BY MR. GALVIN: 12:16:51

Q. Separate and apart from the patent specification, in November of 1998, what is your understanding of how one of skill in the art would have understood the term "network packet data volume"? 12:17:00 12:17:03 12:17:08 12:17:11 12:17:15

MR. POLLACK: Objection. Lacks foundation. 12:17:15

BY MR. GALVIN: 12:17:15

Q. The ordinary meaning of it? 12:17:17

MR. POLLACK: Objection. Lacks foundation, 12:17:20

vague and ambiguous, assumes facts. 12:17:23

THE WITNESS: In the context of the claim 12:17:26

or -- 12:17:26

BY MR. GALVIN: 12:17:26

Q. Just the term. 12:17:29

A. Just the ordinary meaning? 12:17:30

Q. Separate from the patent. Assuming you've 12:17:31

never seen the patent. 12:17:35

MR. POLLACK: Objection. Vague and 12:17:37

ambiguous. 12:17:44

THE WITNESS: The -- in a vacuum, a lot of 12:17:45

these terms are rather -- just without reference to 12:17:47

the patent or anything, a network packet by '98 was 12:17:52

typically associated with an IP packet as opposed to 12:17:59

an Ethernet frame. That could be one way one of 12:18:03

ordinary skill might have considered, again, 12:18:10

considering the term in a vacuum, might have jointly 12:18:12

identified anything in that frame with the notion of a 12:18:17

network packet. The expression "network packet data 12:18:22

volume" could be the number of packets, could be the 12:18:27

number of bytes, total number of bytes that the packet 12:18:33

constitute that are -- that is to say, the data 12:18:47

volume, hyphenated, of a network packet. 12:19:02

BY MR. GALVIN: 12:19:02

Q. Are you finished that? 12:19:17

A. I believe so, yeah. 12:19:20

Q. Okay. Let's change subjects here a bit. 12:19:22

MR. POLLACK: If we're going to change subjects, it's 20 after 12:00. 12:19:30 12:19:32

MR. GALVIN: Do you want to break for lunch? 12:19:34

THE WITNESS: Is that okay? 12:19:36

MR. GALVIN: Yes. 12:19:37

THE VIDEOGRAPHER: We're going off the record. The time is 12:19 p.m. 12:19:38 12:19:40

(Lunch recess taken from 12:19 to 12:23 p.m.) 12:19:44

that definition, would you agree that EMERALD 1997 describes deploying a plurality of network monitors in the enterprise network? 16:40:01 16:40:06 16:40:08

MR. POLLACK: Objection. Vague and ambiguous. 16:40:10 16:40:14

THE WITNESS: Pardon me a second. So I'm looking at the first paragraph, section III, and this is essentially talking about the network service monitor in the context, at the end of this paragraph, service analysis. And it makes reference to reading activity logs and actively probing to supplement normal event gathering. 16:40:38 16:41:12 16:41:25 16:41:27 16:41:30 16:41:59 16:42:04

The implication may be that their real-time analysis of infrastructure and services, that that might encompass network traffic data. But it's not made explicitly at this point here. 16:42:20 16:42:28 16:42:40 16:42:43

So I'm just reluctant to make the connection between a network monitor as construed in the patent by SRI in the claim construction, explicitly make the connection between a network monitor and what they call a service monitor in the EMERALD '97 paper at this point. 16:43:06 16:43:10 16:43:13 16:43:22 16:43:26 16:43:33

BY MR. GALVIN: 16:43:33

Q. So you can't answer my question, or you don't know or -- 16:43:34 16:43:37

MR. POLLACK: Objection. 16:43:38
BY MR. GALVIN: 16:43:38
Q. What would be a fair way to characterize? 16:43:39
A. To be honest with you, I didn't until this point think about applying these claim construction terms to the EMERALD '97 paper. 16:43:42 16:43:45 16:43:49
BY MR. GALVIN: 16:43:49
Q. Well, you understand this is one of the defendants' lead references and arguments as to why the defendants believe the patents are invalid, correct? 16:43:52 16:43:55 16:43:58 16:44:01
MR. POLLACK: Objection. Argumentative, vague and ambiguous. 16:44:01 16:44:04
THE WITNESS: I do understand that, yes. 16:44:05
BY MR. GALVIN: 16:44:05
Q. And you offered opinions with respect to a variety of issues with respect to the EMERALD 1997 paper as to why it did not satisfy certain limitations of the claims, correct? 16:44:08 16:44:10 16:44:13 16:44:17
MR. POLLACK: Objection. The record speaks for itself. 16:44:19 16:44:22
THE WITNESS: I gave specific instances, yeah, examples in my report; for example, in paragraph 23. 16:44:30 16:44:32 16:44:35
BY MR. GALVIN: 16:44:35

Q. And I did not see a specific place in your report where you stated that the EMERALD 1997 paper did not describe deploying a plurality of network monitors in the enterprise network. And what I'm trying to understand is, is it your opinion that that limitation is satisfied or not satisfied? 16:44:36 16:44:40 16:44:44 16:44:47 16:44:50 16:44:55

MR. POLLACK: Objection. Vague and ambiguous. 16:44:58 16:45:10

THE WITNESS: It's clearly, in its language, referring to service, a plurality of service monitors that feed into domain and, in turn, feed into enterprise monitors. 16:45:10 16:45:13 16:45:17 16:45:22

BY MR. GALVIN: 16:45:22

Q. And in fact has some of the very same figures from the patent, correct? 16:45:24 16:45:27

MR. POLLACK: Objection. Argumentative, record speaks for itself. 16:45:29 16:45:30

THE WITNESS: I agree. I believe the figures, figures 1 and 2 are taken from the patent. 16:45:35 16:45:37

BY MR. GALVIN: 16:45:37

Q. And therefore, applying -- based on EMERALD 1997, which you've reviewed and offered opinions on, applying SRI's construction that: 16:45:40 16:45:43 16:45:48

"A network monitor is a process or a component in a network that can 16:45:49 16:45:52

analyze data. Depending on the context and specific claims the network monitor may analyze network traffic data, reports of suspicious network activity or both. Service monitors, domain monitors and enterprise monitors are examples of network monitors." 16:45:53 16:45:57 16:45:59 16:46:02 16:46:04 16:46:06 16:46:09 16:46:13

Applying that construction, wouldn't you agree that EMERALD 1997 describes deploying a plurality of network monitors in the enterprise network, based on that construction? 16:46:14 16:46:15 16:46:19 16:46:20

MR. POLLACK: Objection. Argumentative. Vague and ambiguous. 16:46:23 16:46:26

THE WITNESS: I guess I don't know whether the -- what the authors had in mind when they phrased the first paragraph of section III, and whether that's reflected in our SRI construction -- our construction of the SRI construction of the term "network monitor." I'm just having -- it's -- I don't know. 16:46:56 16:47:06 16:47:09 16:47:18 16:47:24 16:47:29

BY MR. GALVIN: 16:47:29

Q. Well -- 16:47:39

A. It's clearly talking about a plurality of monitors deployed in a network, but I don't know that they are the -- that what the authors had in mind at 16:47:41 16:47:45 16:47:48

this point are network monitors as construed by SRI. 16:47:52

Q. You understand, do you not, that -- 16:47:57

A. That service monitors -- I mean to say that service monitors are analyzing network traffic data. I'm just reading the end of that first paragraph, and I'm -- it doesn't really call that out explicitly, is all I'm pointing out. Section III, there is no page number, so I'm calling out the Bates, 68833, first paragraph of section III. I'm just saying I don't see it explicitly called out that it's looking at network traffic data. You can make inferences, potentially, but I don't see it explicitly called out, is all I'm saying. 16:48:00 16:48:03 16:48:12 16:48:18 16:48:22 16:48:27 16:48:32 16:48:35 16:48:39 16:48:43 16:48:47

Q. EMERALD 1997 is describing the same system that is described in the -- perhaps at an earlier stage, but describing the same system and work that's reflected in the specification of the patents in suit, correct? 16:48:50 16:48:56 16:49:02 16:49:04 16:49:06

MR. POLLACK: Objection. Vague and ambiguous, lacks foundation, assumes facts. 16:49:07 16:49:09

THE WITNESS: I don't know that I would call it the same system. It's referring to something that they call EMERALD at this point. I don't know that I would call it the same system that ultimately became the operational or the EMERALD release or the first 16:49:12 16:49:13 16:49:19 16:49:28 16:49:35

EMERALD release, that it's a fair statement to say that it's the same system that I'm reading in the EMERALD '97 paper. 16:49:38 16:49:42 16:49:47

BY MR. GALVIN: 16:49:47

Q. Do you think it has a relationship to the work that is described in the patents in suit? 16:49:48 16:49:50

A. As you pointed out, figures 1 and 2 are in this paper. So I think that it has a relationship to the preferred embodiment. But I don't believe that the -- that many of the important details nor the claims are in this paper, are disclosed in this paper. 16:49:56 16:49:59 16:50:02 16:50:18 16:50:22

Q. You are aware, correct, that substantial portions of the text of the specification can be found either literally identically or very similar language from the EMERALD 1997 paper? 16:50:30 16:50:33 16:50:37 16:50:42

MR. POLLACK: Objection. Argumentative, assumes facts, vague and ambiguous. 16:50:44 16:50:46

THE WITNESS: I didn't -- I mean I can't attest to the degree to which the word "substantial," and interpret the word "substantial" as important. I wouldn't do that. But clearly, I mean you can just see visual figures 1 and 2 are in the patent specification, and at a minimum associated text describing those figures I expect would be very similar. 16:50:50 16:50:55 16:51:08 16:51:10 16:51:13 16:51:16 16:51:20 16:51:23

BY MR. GALVIN: 16:51:23

Q. Have you compared side by side the text of 16:51:23
the patent specification with the text of EMERALD '97 16:51:28
to identify the similarities and differences? 16:51:30

A. Precisely, a head-to-head comparison, no, 16:51:32
that wasn't done. I didn't do that. I didn't read 16:51:36
the EMERALD '97 paper and see exactly verbatim what 16:51:39
appeared in the patent spec. 16:51:43

Q. Did you review the comparison that was 16:51:48
attached in Mr. Heberlein's expert report showing 16:51:51
highlighted text between the EMERALD 1997 paper and 16:51:54
the specification that was identical or similar? 16:52:00

A. I recall that, yes. I recall. 16:52:04

Q. Let me hand you what's been marked as 16:52:07
Exhibit 26, which is a highlighted copy of the '338 16:52:10
patent specification, which was attached to the 16:52:16
Heberlein expert report. And if we can mark as 16:52:20
Exhibit 27 a highlighted copy of the EMERALD article 16:52:25
with cross-references to the specification, which was 16:52:29
also attached to the Heberlein expert report. 16:52:33

MR. POLLACK: Counsel, do you recall what the 16:52:38
exhibit numbers to the Heberlein report were? 16:52:39

MR. GALVIN: I do not. 16:52:41

(Defendants' Exhibit 27 was marked for 16:52:44
identification.) 16:52:44

THE WITNESS: You gave me two. So exhibits 25 and 27 are the same except for the highlighting? 16:53:06 16:53:16

BY MR. GALVIN: 16:53:16

Q. Yes, correct. 16:53:19

A. I'll just look at one of them, then, because I'm assuming what's highlighted in one is the same in the other. 16:53:25 16:53:28 16:53:32

BY MR. GALVIN: 16:53:32

Q. I believe this is Exhibit GG in the Heberlein expert report. 16:53:38 16:53:43

MR. POLLACK: Which is GG? Both? 16:53:45

MS. DuBORD BROWN: Both of them. 16:53:48

MR. POLLACK: Oh, both of them are together in Heberlein. 16:53:51 16:53:54

BY MR. GALVIN: 16:53:54

Q. So perhaps if we could start looking at the specification, the highlighted specification. 16:54:22 16:54:26

A. Oh, you want to look at that. 16:54:29

Q. Yes. If you turn to column 3, or maybe we just start at column 1, or we could just start at the figures, I guess. 16:54:31 16:54:34 16:54:39

Figure 2, I think you already identified that figure 2 and figure 3 of the specification have some substantial similarities to figures that appear in the EMERALD 1997 paper, correct? 16:54:40 16:54:43 16:54:46 16:54:48

described localized real-time analysis of infrastructure, e.g. routers or gateways, don't you think that a person of ordinary skill in the art as of November 1997 would have understood that an analysis of routers or gateways would have involved an analysis of network packets, TCP/IP packets? 16:58:42 16:58:45 16:58:51 16:58:53 16:58:58 16:59:02

MR. POLLACK: Objection. Assumes facts, lacks foundation, argumentative. 16:59:08 16:59:10

THE WITNESS: One of ordinary skill would infer from that, that involves real-time analysis of network packets? 16:59:15 16:59:21 16:59:24

BY MR. GALVIN: 16:59:24

Q. Yes. 16:59:25

MR. POLLACK: Same objections. 16:59:29

THE WITNESS: I'm not sure what one of ordinary skill would have taken away from that sentence, but they could have thought that what was in play there could have been, for example, a JiNao type of thing. It could have been audit logs from routers or gateways that was in play at that point. It's kind of vague in the EMERALD '97 paper. 16:59:36 16:59:38 16:59:40 16:59:42 16:59:46 16:59:51 17:00:00

And like I said, if they -- you know, my opinion is if they explicitly wanted to call out real-time analysis of TCP/IP packets, they would have at that point instead of writing what they did. 17:00:04 17:00:07 17:00:13 17:00:16

BY MR. GALVIN: 17:00:16

Q. Do you understand that the standard isn't what the authors intended to convey; the standard for evaluating anticipation is what one skilled in the art would have understood from reading the reference, correct? 17:00:22 17:00:23 17:00:27 17:00:29 17:00:32

A. I understand. 17:00:32

Q. So I want to focus -- I want to keep the focus on your opinions of what one of ordinary skill in the art would have understood based on the disclosure. 17:00:33 17:00:38 17:00:42 17:00:44

MR. POLLACK: Objection. Argumentative. Counsel, stop making speeches and ask questions, please. 17:00:46 17:00:48 17:00:51

THE WITNESS: Considering the existence of the JiNao reference that one of ordinary skill may have read or is presumed to have read, they could have easily taken away from that that examination of other information made available by routers or gateways, rather than simply examination of a raw TCP/IP packet trace, was in play. 17:00:51 17:00:55 17:00:57 17:01:01 17:01:14 17:01:19 17:01:25

So I'm just -- considering that that wasn't known how to precisely do that, how to do that at the time, I'm not sure how you can draw from that that necessarily examination of network packets. 17:01:31 17:01:35 17:01:39 17:01:42

BY MR. GALVIN: 17:01:42

Q. All right. Let's turn -- staying on the EMERALD 1997 reference to page 356, right-hand column, first and second sentence, "Underlying the deployment of an EMERALD monitor is the selection of a target specific event stream." 17:01:48 17:01:50 17:01:59 17:02:04 17:02:06

A. 356? I'm sorry? 17:02:08

Q. Right-hand column. Right-hand column. 17:02:13

A. First paragraph, okay. 17:02:16

Q. "The event stream may be derived from a variety of sources, including audit data, network datagrams, SMNP traffic, application logs and analysis results from other intrusion detection instrumentation." 17:02:17 17:02:20 17:02:23 17:02:26 17:02:28 17:02:31

Do you agree that one of ordinary skill in the art in November of 1997 reading this reference would have understood the term "network datagrams" in this context to refer to analyzing and generating, deriving an event stream from network packets? 17:02:32 17:02:35 17:02:39 17:02:45 17:02:50

MR. POLLACK: Objection. Vague and ambiguous, lacks foundation. 17:02:55 17:02:56

THE WITNESS: A network datagram would have been understood at this point to be an IP packet. So that is an example of information that one of ordinary 17:03:07 17:03:11 17:03:18

skill -- I mean just reading it there, IP datagrams. 17:03:24

BY MR. GALVIN: 17:03:24

Q. Would you agree, therefore, that EMERALD 1997 disclosed to one of ordinary skill in the art in -- prior to November 1997 that the EMERALD system could be used to derive event streams by monitoring network packets? 17:03:30 17:03:36 17:03:40 17:03:47 17:03:52

MR. POLLACK: Objection. Vague and ambiguous, lacks foundation. 17:03:52 17:03:55

THE WITNESS: Well, I think -- first of all, I don't think the writing of -- I don't think by the time of this paper's publication that EMERALD was, in fact, a system. In fact, it largely reads as a proposal, and therefore, I would say that one of ordinary skill would feel that the -- it's possible that the intent of the EMERALD system that was to be developed was to consider examination of network datagrams, of IP packets at the -- it doesn't say service monitor in this context, but I'm assuming at the service monitor level. 17:03:56 17:04:01 17:04:11 17:04:14 17:04:22 17:04:27 17:04:36 17:04:45 17:04:50 17:04:57 17:05:03

So I'm not sure that I would characterize it, as one of ordinary skill, the EMERALD system looks at network datagrams. I think it's written very much like a proposal. It says "may be derived." I think I would infer that they're examining audit data, SNMP 17:05:06 17:05:09 17:05:13 17:05:17 17:05:28

traffic, application logs. It's sort of telling what isn't highlighted, item 15 in the EMERALD '97 paper. 17:05:34 17:05:39

So I believe one of ordinary skill would understand that EMERALD -- that the EMERALD project would -- will consider employing network datagram information for the purposes of intrusion detection. 17:05:50 17:05:52 17:05:55 17:06:04

BY MR. GALVIN: 17:06:04

Q. And the network datagram information would be network packets? 17:06:06 17:06:09

A. It would be IP packets. The word "datagram" is typically used at the time to connote an IP packet. 17:06:10 17:06:11

Q. Turn to page 364 -- 17:06:49

A. Okay. 17:06:56

Q. -- under the heading "Related Intrusion Detection Research." If you go to the top right-hand column, under that section, it says, "Various other efforts have considered one of the two types of analysis -- signature-based (e.g, Porras [18] has used a state-transition approach." 17:06:57 17:07:01 17:07:03 17:07:08 17:07:12 17:07:15

A. I hate to tell you -- 354, you said? 17:07:18

Q. 364. 17:07:21

A. Oh, 364, sorry. 17:07:23

Q. "Various other efforts have considered one of the two types of analysis -- signature-based, (e.g. Porras [18] has 17:07:33 17:07:35 17:07:37

used a state-transition approach; the U.C. Davis and Trident DIDS addresses abstracted analysis for networking but not scalability. The Network Security Monitor [7] seeks to analyze packet data rather than conventional audit trails." 17:07:40 17:07:44 17:07:47 17:07:48 17:07:51 17:08:01 17:08:01

Do you see that? 17:08:01

A. Right. I see that. I read that. 17:08:01

Q. As an author of scientific publications such as this, what is the purpose of citing references and referring readers to work that might be related? 17:08:11 17:08:14 17:08:18

MR. POLLACK: Objection. Vague and ambiguous, overly broad, lacks foundation. 17:08:22 17:08:23

THE WITNESS: The purpose? It's just generally speaking important to talk about prior publications that are relevant to your paper so that you can more clearly delineate what is novel, what is different between what they have done and what you have done, what you are planning to do. 17:08:31 17:08:40 17:08:43 17:08:54 17:09:00 17:09:02

In this case, this is, again, not a typical research article. But you know, typically when you have a scholarly paper, there is a significant section on related background research to more clearly designate and delineate what you're doing and the 17:09:05 17:09:08 17:09:11 17:09:16 17:09:23

novelty of what you're doing compared to what's been going on in the past. 17:09:25 17:09:28

BY MR. GALVIN: 17:09:28

Q. And by making citations to related work, the authors are able to direct the reader to prior work in a way that would avoid the author having to re-say everything that's already been said in the art, correct? 17:09:29 17:09:33 17:09:38 17:09:43 17:09:46

MR. POLLACK: Objection. Vague and ambiguous, lacks foundation. 17:09:46 17:09:47

THE WITNESS: Sure. Sometimes a reference is used in a summary way, if it's -- sometimes it's merely stating that it's in the general space of publications, general space of subject matter. Also informs the reader indirectly that the authors are aware of these papers, that they have -- they're familiar with these papers. But yeah, sometimes a paper, a citation is used as a proxy for an explanation -- 17:09:52 17:10:03 17:10:09 17:10:13 17:10:20 17:10:23 17:10:27 17:10:36 17:10:39

BY MR. GALVIN: 17:10:39

Q. If one -- 17:10:40

A. -- instead of an explanation. 17:10:44

Q. If one skilled in the art back in October of 1997 was reading the EMERALD 1997 paper and was interested in applying the teachings of the EMERALD 17:10:47 17:10:52 17:10:56

1997 paper in order to analyze packet data rather than conventional audit trails, would one of skill in the art have been motivated to look to the network security monitor reference 7 that is cited in the EMERALD 1997 paper? 17:11:00 17:11:06 17:11:13 17:11:18 17:11:20

MR. POLLACK: Objection. Lacks foundation, vague and ambiguous, calls for speculation. 17:11:21 17:11:25

THE WITNESS: Again, I can't anticipate what a person of ordinary skill at the time would have done equipped with this, but the paper makes direct reference to NSM as an approach, again using the quote, that seeks to analyze packet data. 17:11:32 17:11:33 17:11:38 17:11:42 17:11:45

And referring back to where we were previously, I believe it was your item highlighted 15, where the EMERALD authors intend to examine intrusion detection based on network datagrams, which I would -- could be -- again, NSM operates in a LAN, and it could be that that -- that one of ordinary skill would think that the EMERALD investigators will examine NSM as a first step, perhaps, or they already knew NSM, the NSM technique, the NSM method. 17:11:49 17:11:51 17:12:10 17:12:14 17:12:19 17:12:28 17:12:32 17:12:38 17:12:43

Beyond that, I mean I'm not sure what one of ordinary skill would do or -- 17:12:47 17:12:52

BY MR. GALVIN: 17:12:52

Q. Would you agree that if a person of ordinary 17:12:59

skill in the art was interested in finding out more about analyzing packet data, that EMERALD 1997 directed the reader to look to the network security monitor reference 7? 17:13:02 17:13:05 17:13:08 17:13:12

MR. POLLACK: Objection. Vague and ambiguous. The paper speaks for itself. 17:13:14 17:13:17

THE WITNESS: To the extent that EMERALD '97 calls out NSM and states that it, quote, seeks, unquote, to analyze packet data, I would agree. 17:13:19 17:13:23 17:13:30

BY MR. GALVIN: 17:13:30

Q. Were denial of service attacks well known in the art as of November 1997? 17:14:13 17:14:16

MR. POLLACK: Objection. Vague and ambiguous in many respects. 17:14:20 17:14:23

THE WITNESS: Certain denial of service attacks were known at the time. 17:14:26 17:14:28

BY MR. GALVIN: 17:14:28

Q. Were SYN flooding attacks known prior to November of 1997? 17:14:32 17:14:37

MR. POLLACK: Objection. Vague and ambiguous, lacks foundation. 17:14:40 17:14:41

THE WITNESS: Yes, I believe so. Generally speaking, it's a large family of attacks. Some were called out in the literature. 17:14:42 17:14:45 17:14:51

BY MR. GALVIN: 17:14:51

Q. Would one of ordinary skill in the art in -- as of November of 1997 have known to monitor SYN packets for suspicious activity or the number of SYN packets to SYN ACK packets if that person sought to detect SYN flood attacks? 17:14:54 17:15:01 17:15:07 17:15:10 17:15:18

MR. POLLACK: Objection. Vague and ambiguous, lacks foundation. Compound, sorry. 17:15:20 17:15:21

THE WITNESS: I'm not sure. I'm not sure that -- when you say "look at," how is the one of ordinary skill looking at this traffic? In what context, is what I'm asking. 17:15:44 17:15:58 17:16:10 17:16:13

BY MR. GALVIN: 17:16:13

Q. Suppose a person of ordinary skill in the art had been presented with the problem, detect SYN floods. Would it have been known to a person of ordinary skill in the art who was setting out to address that problem that the way -- one way to achieve that would be to monitor the number of SYN packets and compare that to the number of SYN ACK packets? 17:16:15 17:16:17 17:16:22 17:16:28 17:16:31 17:16:35 17:16:39 17:16:42

MR. POLLACK: Objection. Vague and ambiguous, lacks foundation. 17:16:43 17:16:45

THE WITNESS: It's not clear to me that one of ordinary skill would have -- I mean you're assuming that there's a system in place that would allow them 17:16:49 17:16:51 17:17:21

to examine packet traffic. 17:17:25
BY MR. GALVIN: 17:17:25
Q. Okay. Let's start with that. In November 17:17:28
of 1997, were there tools available that would have 17:17:30
allowed one of ordinary skill in the art to measure 17:17:37
the number of SYN packets and compare -- and measure 17:17:40
the number of SYN ACK packets? 17:17:40
MR. POLLACK: Objection. Lacks foundation, 17:17:42
incomplete hypothetical, vague and ambiguous. 17:17:44
THE WITNESS: It's possible that some systems 17:17:54
existed that would have presented a system 17:18:00
administrator, if they were suitably configured, with 17:18:06
information along those lines. I mean whether one of 17:18:12
ordinary skill would have -- for the purposes of SYN 17:18:31
flood detection, you're asking would they have -- I'm 17:18:37
not sure. I'm not sure what you're asking. Like 17:18:47
equipped with a specific system? 17:18:49
BY MR. GALVIN: 17:18:49
Q. Well, would they have known that a SYN flood 17:18:51
was an attack in which the number of SYN packets 17:18:55
exceeded the number of SYN ACK packets? 17:18:58
MR. POLLACK: Objection. Lacks foundation, 17:19:00
vague and ambiguous. 17:19:02
THE WITNESS: It's -- I'm not sure. That 17:19:14
specific example, I'm not sure. They would have known 17:19:16

we want to take a brief break? 17:31:30

MR. GALVIN: Sure. 17:31:33

THE VIDEOGRAPHER: We're going off the record, the time is 5:31 p.m. 17:31:34 17:31:35

(Break taken from 5:31 to 5:38 p.m.) 17:31:41

THE VIDEOGRAPHER: We're back on the record. The time is 5:38 p.m. 17:37:26 17:38:16

BY MR. GALVIN: 17:38:16

Q. Mr. Kesidis, if you could turn back to Exhibit 3, your expert report regarding EMERALD, paragraph 30. The first sentence, you wrote: 17:38:24 17:38:34 17:38:38

"In fact, it is not at all clear what one of ordinary skill in the art in 1997 would choose firewall logs as an input to an intrusion detection system." 17:38:44 17:38:47 17:38:48 17:38:51 17:38:53

And the last sentence said: 17:38:55

"As firewall logs contain information about packets that are not on the network, one of ordinary skill would not be tempted to use this information to detect network intrusions." 17:38:57 17:39:00 17:39:02 17:39:04 17:39:06 17:39:08

What's the basis for that opinion? 17:39:09

A. So the context here is -- the context of the 17:39:13

patents is a network-based intrusion detection system examining network traffic and trying to detect alerts, based on network traffic, detect attacks based on network traffic. So the firewall logs, the firewalls themselves will filter packets that are not observed, and the packets that are filtered are, at the time of '97, the subject of, I would say, the very simple rules that are in play in a firewall. 17:39:23 17:39:47 17:39:59 17:40:06 17:40:20 17:40:23 17:40:27 17:40:34

So if I have a network-based intrusion detection system examining network data traffic, I'm not sure that I would simultaneously examine firewall logs of packets that were filtered out of the network. 17:40:42 17:40:48 17:40:58 17:41:04

Q. Do you understand that would be an unusual approach as of November 1998? 17:41:19 17:41:21

MR. POLLACK: Objection. Vague and ambiguous. 17:41:25 17:41:27

THE WITNESS: Again, the context of this is a new network intrusion detection system that would examine network datagrams. And it's -- I'm just trying to think if one of ordinary skill would understand a firewall as simply checking packets against a list of relatively simple rules. And those packets that are nevertheless passed through the firewall would be the subject of examination of an intrusion detection system based on the network. 17:41:41 17:41:46 17:41:59 17:42:23 17:42:25 17:42:34 17:42:41 17:42:51 17:42:59

The firewall doesn't log pass-through packets typically at the time of '97. It typically logs those packets that are blocked. Firewall information could be used in intrusion detection systems, but I was making reference to, here, the -- let's see, in reading the '97 paper, audit logs -- again, if I look at the EMERALD '97, the general architecture that's called out, the hierarchical architecture that's called out in '97, it's not clear to me that the new work to be done that's being proposed in this, that it doesn't seem to be highlighting, notwithstanding our previous discussion, the use of firewall audit logs. It's mentioning them as a potential source of information only parenthetically. 17:43:03 17:43:08 17:43:13 17:43:30 17:43:36 17:43:56 17:44:15 17:44:19 17:44:22 17:44:28 17:44:34 17:44:41 17:44:44 17:44:49

And I think that, again, if I'm -- if I've got a network service monitor examining datagrams, I wouldn't appeal to a firewall audit log, because -- to get that information, because it would be an audit log. It wouldn't be real-time. It would inform me typically of what packets it blocked, not the packets that it passed through. 17:44:56 17:45:01 17:45:13 17:45:17 17:45:21 17:45:24 17:45:28

BY MR. GALVIN: 17:45:28

Q. As of October 1997, firewalls logged packets that had been blocked, correct? 17:45:36 17:45:47

MR. POLLACK: Objection. Overly broad, vague 17:45:50

and ambiguous, lacks foundation. 17:45:55

THE WITNESS: You could -- my understanding is you could configure them to record what they had blocked. 17:45:56 17:45:59 17:46:03

BY MR. GALVIN: 17:46:03

Q. And would the blocked packets be a measure of network connection denials? 17:46:03 17:46:07

MR. POLLACK: Objection. Vague and ambiguous, lacks foundation. 17:46:10 17:46:12

THE WITNESS: They would have been -- the packets would have been denied entry by the firewall, so I'm -- whether they were a connection attempt or could have been a connection, could have been interpreted as a connection attempt, but not necessarily so. 17:46:22 17:46:23 17:46:28 17:46:41 17:46:43 17:46:53

BY MR. GALVIN: 17:46:53

Q. If you could look at the '212 patent, which is Exhibit 7. 17:46:59 17:47:02

A. Okay. 17:47:14

Q. Claim 1. Would you agree that the EMERALD 1997 paper described deploying a plurality of network monitors in the enterprise network? 17:47:14 17:47:18 17:47:25

MR. POLLACK: Objection. Asked and answered repeatedly. 17:47:28 17:47:30

THE WITNESS: Again, it's this issue of 17:47:32

construing a network monitor as is construed by us in Exhibit 8, as what's described in the EMERALD '97 paper. But a plurality of EMERALD service monitors as defined in the EMERALD '97 paper or suggested in the EMERALD '97 paper? 17:47:35 17:47:46 17:47:55 17:48:00 17:48:06

BY MR. GALVIN: 17:48:06

Q. Doesn't the EMERALD 1997 paper not only describe plurality of service monitors but also domain monitors and enterprise monitors? 17:48:08 17:48:11 17:48:14

MR. POLLACK: Objection. Lacks foundation, vague and ambiguous. 17:48:16 17:48:29

THE WITNESS: Implicitly, yes, in page 356. 17:48:29

BY MR. GALVIN: 17:48:29

Q. Or explicitly, correct? 17:48:33

MR. POLLACK: Objection. Vague and ambiguous, lacks foundation. 17:48:35 17:48:36

THE WITNESS: What are you referring to? 17:48:40

BY MR. GALVIN: 17:48:40

Q. "A domain monitor is responsible for surveillance over all or part of a domain." Page 356. 17:48:41 17:48:46 17:48:49

A. I'm there, yeah. So your question was it teaches a plurality of domain monitors? 17:48:50 17:48:55

Q. Well, let's continue on, page 357, top right column: "All EMERALD monitors (service, domain and 17:48:58 17:49:01

enterprise) are implemented using the same monitor code base." 17:49:04 17:49:08

MR. POLLACK: Objection. Vague and ambiguous, if there is a question pending. 17:49:14 17:49:15

THE WITNESS: So by that I'm supposed to assume that there were multiple domain monitors? I'm sorry, you said explicitly. 17:49:17 17:49:19 17:49:22

BY MR. GALVIN: 17:49:22

Q. I read EMERALD 1997 as describing service monitors, domain monitors and enterprise monitors in the context of the EMERALD system. There are figures describing the monitor architecture, and when you look at the comparison between EMERALD 1997 paper and the '338 patent specification that you have in front of you, the sections that are describing what the monitors are, and the hierarchy of monitors have substantial portions in column 3 and column 4, for example, of code that -- of text that is very, very similar, if not identical, between the two references. 17:49:29 17:49:32 17:49:36 17:49:39 17:49:42 17:49:46 17:49:50 17:49:53 17:49:57 17:50:00 17:50:05 17:50:05

Based on all of that, would you agree that the EMERALD 1997 paper describes deploying a plurality of network monitors in the enterprise network? 17:50:09 17:50:14 17:50:20

MR. POLLACK: Objection. Vague and ambiguous, overly broad, mischaracterizes the record, 17:50:23 17:50:24

lacks foundation, argumentative. 17:50:28

THE WITNESS: I'm not sure I'd characterize it as very, very similar. There is some text that's identical and some text that's important, that's different in important ways. But yeah, I'll concede that -- well, I'm not a hundred-percent sure, but I'll concede that the EMERALD '97 paper teaches a plurality of domain monitors. 17:50:32 17:50:35 17:50:38 17:50:41 17:50:44 17:50:49 17:50:52

BY MR. GALVIN: 17:50:52

Q. And so therefore, would you agree that EMERALD 1997 describes deploying a plurality of network monitors in the enterprise network using SRI's construction of network monitors? 17:50:54 17:50:57 17:51:08 17:51:08

MR. POLLACK: Objection. Asked and answered repeatedly. Still vague and ambiguous. 17:51:08 17:51:10

THE WITNESS: Again, I don't think EMERALD '97 teaches a -- let me remind myself where you were. I just want to make sure -- explicitly teaches a network monitor as is called out in the SRI construction of the claim in Exhibit 8. 17:51:15 17:51:18 17:51:31 17:51:31 17:51:37

BY MR. GALVIN: 17:51:37

Q. What is missing? 17:51:39

MR. POLLACK: Objection. Let the witness finish. And vague and ambiguous. 17:51:40 17:51:42

THE WITNESS: Okay. So I'm just looking for 17:52:07

the section. Sorry. I recall now, you called out highlight 15. You're saying that the event stream could be built from network datagrams. May be derived. So a hypothetical EMERALD monitor, okay, if I interpret a hypothetical EMERALD monitor as one that directly examines network datagrams and builds an event stream from them in the context of this paper, then yeah, the deploying step -- the deploying step would be there. 17:52:09 17:52:18 17:52:21 17:52:25 17:52:33 17:52:37 17:52:46 17:52:54 17:53:08

BY MR. GALVIN: 17:53:08

Q. What about the step detecting by the network monitors suspicious network activity based on analysis of network traffic data wherein at least one of the network monitors utilizes a statistical detection method. Is that describe in the EMERALD 1997 reference, in your opinion? 17:53:08 17:53:11 17:53:14 17:53:17 17:53:20 17:53:23

MR. POLLACK: Objection. Vague and ambiguous. 17:53:26 17:54:07

THE WITNESS: The intent, again, in -- around highlight 21 in Exhibit 27 is that the monitor generates reports of suspicious reports or intrusions. I don't know where it talks about a statistical detection method in this EMERALD '97 paper offhand. 17:54:08 17:54:17 17:54:25 17:54:45 17:54:53

BY MR. GALVIN: 17:54:53

Q. Figure 1 at page 357. 17:54:56

A. Right. It has mention of a profiler engine. 17:55:01
Q. And at page 359. 17:55:15
A. Okay. I can see that it's advocating -- it's explaining a statistical anomaly detection method, is what it's defining as the profiler engine. 17:55:53 17:55:59 17:56:05
Q. So therefore, would you agree that the EMERALD 1997 paper describes detecting by the network monitors suspicious network activity based on analysis of network traffic data, wherein at least one of the network monitors utilizes a statistical detection method? 17:56:09 17:56:11 17:56:15 17:56:17 17:56:20 17:56:24
MR. POLLACK: Objection. Vague and ambiguous, lacks foundation. 17:56:25 17:56:26
THE WITNESS: I would say it describes an intent, not a practice. 17:56:30 17:56:34
BY MR. GALVIN: 17:56:34
Q. Well, are you saying that one skilled in the art in October 1997 would not have been able to implement a statistical detection method after reading EMERALD 1997 paper and based on the state of the prior art at that time? 17:56:41 17:56:44 17:56:49 17:56:54 17:56:58
MR. POLLACK: Objection. Vague and ambiguous, lacks foundation. 17:56:59 17:57:01
THE WITNESS: I don't believe that -- it's very -- it essentially says it's going to begin with 17:57:34 17:57:52

the generic techniques used by NIDES in the previous paragraph to that highlighted 17, 18. 17:57:55 17:58:14

The paragraph at the end of page 359: 17:58:25

"While NIDES/Stats has been reasonably successful profiling users' later applications, it will be extended to the more general subject class typography required by EMERALD," 17:58:28 17:58:30 17:58:32 17:58:34 17:58:35

claims that at this point, EMERALD '97 paper, that "the underlying mechanisms," by inference, of NIDES, "are well suited to the problem of network anomaly detection, with some adaptation." 17:58:38 17:58:44 17:58:49 17:58:50

But I just don't -- my opinion is that this passage on page 359, Section C, gives sufficient information to one of ordinary skill on how to do this. 17:59:00 17:59:03 17:59:13 17:59:15

BY MR. GALVIN: 17:59:15

Q. And when you say "this," are you referring to implementing the long-term and short-term statistical profiling techniques that are -- were described in NIDES and adapted as described in the specification of the patents in suit? 17:59:16 17:59:19 17:59:22 17:59:26 17:59:30

MR. POLLACK: Objection. Mischaracterizes the record, mischaracterizes the testimony, vague and ambiguous. 17:59:31 17:59:33 17:59:47

THE WITNESS: I believe, yeah, that's what I meant, roughly speaking. The -- there are some -- apart from the intent of adapting the rough, generic statistical detection approach used in NIDES, in this context, the author has identified that it's a different context. The adaptation will not be straightforward. 17:59:47 17:59:49 17:59:59 18:00:07 18:00:09 18:00:12 18:00:18

Like I said, I'm reading this largely, in particular this section, as a research proposal, almost. 18:00:22 18:00:26 18:00:30

BY MR. GALVIN: 18:00:30

Q. Now, yesterday I thought when we -- or Friday when we discussed statistical detection method, it was my understanding that it was your position that the term "statistical detection method" in claim 1 of the '212 patent was not limited to the long-term and short-term statistical profiles that are claimed in the '338 patent. Is that a fair statement of your position? 18:00:31 18:00:34 18:00:38 18:00:40 18:00:43 18:00:47 18:00:51 18:00:54

A. Yes, I would say. 18:00:56

Q. Okay. Now, you've said that the EMERALD 1997 paper did not enable this adapting the long-term statistical and short-term statistical profile techniques of NIDES. But are you saying that in November of -- or October of 1997, one skilled in the 18:00:57 18:01:02 18:01:09 18:01:12 18:01:16

art reading EMERALD 1997 would have known of no other statistical detection methods that could be utilized in connection with monitoring network traffic data? 18:01:23 18:01:28 18:01:34

MR. POLLACK: Objection. Lacks foundation, vague and ambiguous. 18:01:39 18:01:40

THE WITNESS: In my opinion, a statistical detection method is one that involves a decision made using random, uncertain information. And one of ordinary skill, as we defined it, had an undergraduate degree in electrical engineering or computer engineering and could have taken a statistical detection -- could have taken a course where stats was covered and may have seen specific techniques other than those specifically employed in NIDES to perform detection. 18:01:55 18:01:57 18:02:12 18:02:21 18:02:25 18:02:28 18:02:31 18:02:33 18:02:36 18:02:45

I'm not sure I understand. You're saying would one of ordinary skill have been tempted to do something other than what's generically called out in NIDES? 18:02:51 18:02:57 18:03:01 18:03:04

BY MR. GALVIN: 18:03:04

Q. Yes. Would they have been able to? 18:03:04

MR. POLLACK: Objection. Vague and ambiguous, lacks foundation. 18:03:06 18:03:08

THE WITNESS: I don't believe -- I mean roughly speaking, I don't believe so. 18:03:08 18:03:10

BY MR. GALVIN: 18:03:10

Q. Okay. So if that's the case in October of 1997, we have the specification which is filed in November of 1998. The only statistical detection technique that is disclosed in the specification, as we covered on Friday, was the long-term and short-term statistical profile technique; is that correct? 18:03:15 18:03:19 18:03:23 18:03:28 18:03:31 18:03:36 18:03:38

MR. POLLACK: Objection. Mischaracterizes the testimony, lacks foundation. 18:03:38 18:03:40

THE WITNESS: I mean I'm not sure I specifically recall what was said on Friday. 18:03:42 18:03:44

BY MR. GALVIN: 18:03:44

Q. Are there other methods other than the long-term and short-term statistical profile techniques that were described in the specification? 18:03:47 18:03:50 18:03:52

MR. POLLACK: Same objections. 18:03:57

THE WITNESS: I believe that the specification discusses threshold-based techniques in the statistical context, but we covered this before, and I'm misremembering where in the patent that may have been discussed. Certainly the prominent statistical detection technique in the patent specification is one involving a long and short-term statistical profile. 18:04:44 18:04:45 18:04:51 18:04:57 18:05:00 18:05:12 18:05:14 18:05:18